UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,016	05/10/2006	Vesa Torvinen	P18450US1	1254

27045 7590 12/08/2009

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
BENOIT, ESTHER	

ART UNIT	PAPER NUMBER
2442	

MAIL DATE	DELIVERY MODE
12/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/595,016	TORVINEN ET AL.	
	Examiner	Art Unit	
	ESTHER BENOIT	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 August 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-14,16-20 and 22-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-14,16-20 and 22-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Action is in response to the Amendment filed on August 12, 2009. Claims 1-3, 5-14, 16-20, and 22-33 are pending in this application. Claims 1, 3, 10-11, 16-18, 20, 27, and 29 have been amended. Claims 4, 15, and 21 have been cancelled.

Response to Arguments

2. Applicant's arguments filed August 12, 2009 have been fully considered but they are not persuasive. The applicants are arguing in substance the following:

Arguments under 35 U.S.C. 103 (a)

***Arguments to Claim 1*:**

a) The prior art reference- Tuomi does not disclose a remote server which is separate and different from an authentication server.

b) The prior art reference- Reiche does not disclose sending details of the access request to the home network's authentication node.

b) The prior art reference- Niemi does not disclose generating an HTTP challenge using an algorithm capable of generating end-user passwords, including details of the temporary identity of the end user.

Response to arguments of Claim 1:

As to point a: The argument has been considered but is not persuasive. Tuomi discloses an access controller **(112)** and an authentication server **(114)** where the authentication server creates a userID and password for the user requesting access.

The access controller is responsible for user authentication between the authentication server and the service access point (Col. 3, lines 23-40) The authentication node of the instant application receives request for access and details of the temporary identity for the end user, which is similar to the functions of the access controller in the reference Tuomi.

As to point b: The argument has been considered but is not persuasive. Reiche discloses an authentication server which resides at nodes, where the server receives a request for access from a user's browser (Col. 7, lines 5-10 and Col. 5, lines 12-22).

As to point c: The argument has been considered but is not persuasive. IN the reference Niemi, when a server receives an "auts" parameter, the server generates a new challenge for the client. Information carried in the nonce parameter includes the server information (pg. 7, paragraph 1, "If the server receives...").

As to any claims not specifically discussed, the applicants argued that it was patentable for one of the reasons discussed above. Please see response to above arguments for unspecified discussions.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over of Niemi et al. (RFC 3310, HTTP Digest Authentication Using AKA), in view of Reiche (6,092,196), and further in view of Tuomi et al. (US 7,395,050 B2).

With respect to claim 1, Niemi discloses at the authentication node or the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user password (pg. 6, paragraph 2, "If the server...", and pg. 7, paragraph 1, "When a client...") and at the UE, generating a password based on the HTTP Digest challenge (pg. 7, paragraph 2, "The resulting...") the password being associated with the identity of the remote server and the identity of the UE (pg. 9, "3) Request containing credentials", *where the identity of the server is encoded in the realm*)

Niemi does not disclose sending a request for access from the UE to the remote server; sending to an authentication node in the UE's home network details of the request for access, said details including said temporary identity for the UE; and storing the password and the UE ID at the UE.

However, Reiche discloses sending a request for access from the UE to the remote server; (Col. 5, lines 15-17) and sending to an authentication node in the UE's home network details of the request for access; (Col. 6, lines 52-56) the challenge includes details of the UE ID; (Col. 5, lines 17-25) and storing the password and the UE ID at the UE (Col. 5, lines 25-28, *where the user's browser retains authentication information such as password, user ID, and etc.*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to generate an HTTP Digest challenge based on a request sent to a remote, *because* it will allow the user secure access to the server and recall the credentials for accessing the remote server at a later period.

Niemi and Reiche also do not disclose creating a temporary identity for the UE by the remote server and sending an authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server.

However, Tuomi discloses creating a temporary identity for the UE at the remote server (Col. 10, lines 59-61, *where the ID is created at the authentication server*) and sending an authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server (Col. 11, lines 1-10, *where user uses userID and password created by server to gain access and in turn lets the authentication server know the user has received the access credentials*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Tuomi with the teachings of Niemi and Reiche to create a temporary ID for the end user at the remote server, *because* it will allow the authentication server the ability to append the generated password along with an ID for the user to use when accessing the server.

With respect to claim 18, the limitations of claim 18 are similar to the limitations as claim 1. Therefore, the claim is rejected for the same reasons as claim 1 above. Please see rejection above.

With respect to claim 2, Niemi discloses the method, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA) (pg. 6, paragraph 2, "If the server...", and pg. 7, paragraph 1, "When a client...")

With respect to claim 3, Niemi does not disclose the method, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE.

However, Reiche discloses sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server and wherein the identity of the remote server is stored at the UE Col. 5, lines 25-28, *where the user's browser retains authentication information such as password, user ID, and etc.*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to use the identity of the remote server stored on the end user to generate the HTTP Digest Challenge, *because* it will allow the user secure access to the server and recall the credentials for accessing the remote server at a later period.

With respect to claim 5, Niemi does not disclose the method, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node.

However, Reiche discloses sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to include redirecting the request for access to the authentication node if the client is being authenticated at the authentication node.

With respect to claim 6, the claim is rejected for the same reason as Claim 5 above. In addition, Reiche discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE (Col. 5, lines 17-25)

With respect to claim 7, Niemi discloses the method, wherein the password is stored at the authentication (pg. 6, paragraph 2, "If the server…", and pg. 7, paragraph 1, "When a client…")

With respect to claim 8, the claim is rejected for the same reason as Claim 5 above. In addition, Reiche discloses authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server

after the password has been generated (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

With respect to claim 9, Niemi does not disclose the method, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly.

However, Reiche discloses sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to have the remote server contact the authentication node directly since the password is stored at the authentication node. This allows a more appropriate way for the remote server to contact the authentication node directly and authenticate the client.

With respect to claim 10, Niemi discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server (pg. 7, paragraph 4, "If the server..", lines 1-4)

With respect to claim 11, Niemi discloses the method, wherein the HTTP Digest challenge is generated at the remote server (pg. 7, paragraph 4, "If the server..", lines 1-4)

With respect to claim 12, Niemi discloses the method, further comprising sending the HTTP digest challenge from the remote server to the UE (pg. 7, paragraph 5, "When a client...", line 1)

With respect to claim 13, Niemi discloses a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server (pg. 7, paragraph 5, "When a client.."; pg. 8, paragraph 1, "The AUTN token..")

With respect to claim 14, Niemi discloses authenticating the UE at the authentication node and returning an authentication result to the remote server (pg. 5, paragraph 5, "Using the shared secret..", lines 2-5; paragraph 6, "The authentication response")

With respect to claim 16, Niemi discloses sending an authentication request from the remote server to the authentication node, (pg. 5, paragraph 3, "The server creates..") sending the password from the authentication node to the remote server, (pg. 5, paragraph 5, "Using the shared secret..", lines 2-5; paragraph 6, "The authentication response..") and authenticating the UE at the remote server (pg. 7, paragraph 4, "If the serer receives..", lines 1-2)

With respect to claim 17, Niemi discloses sending an authentication request from the remote server to the authentication node, (pg. 5, paragraph 3, "The server creates..") authenticating the UE at the authentication node, (pg. 5, paragraph 5, "Using the shared..", lines 2-5) and sending confirmation of authentication from the

authentication node to the remote server (pg. 5, paragraph 6, "The authentication response..")

With respect to claim 19, Niemi discloses the method, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA) (pg. 6, paragraph 2, "If the server...", and pg. 7, paragraph 1, "When a client...")

With respect to claim 20, Niemi does not disclose the method, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE.

However, Reiche discloses sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server and wherein the identity of the remote server is stored at the UE (Col. 5, lines 17-25)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to use the identity of the remote server stored on the end user to generate the HTTP Digest Challenge, *because* it will allow the system to know which remote server the client is communicating with.

With respect to claim 22, Niemi does not disclose the method, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node.

However, Reiche discloses sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to include redirecting the request for access to the authentication node if the client is being authenticated at the authentication node.

With respect to claim 23, the claim is rejected for the same reason as Claim 22 above. In addition, Reiche discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE (Col. 5, lines 17-25)

With respect to claim 24, Niemi discloses the method, wherein the password is stored at the authentication (pg. 6, paragraph 2, "If the server...", and pg. 7, paragraph 1, "When a client...")

With respect to claim 25, the claim is rejected for the same reason as Claim 23 above. In addition, Reiche discloses authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

With respect to claim 26, Niemi does not disclose the method, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly.

However, Reiche discloses sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Niemi with the teachings of Reiche to have the remote server contact the authentication node directly since the password is stored at the authentication node. This allows a more appropriate way for the remote server to contact the authentication node directly and authenticate the client.

With respect to claim 27, Niemi discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server (pg. 7, paragraph 4, "If the server..", lines 1-4)

With respect to claim 28, Niemi discloses the method, wherein the HTTP Digest challenge is generated at the remote server (pg. 7, paragraph 4, "If the server..", lines 1-4)

With respect to claim 29, Niemi discloses the method, further comprising sending the HTTP digest challenge from the remote server to the UE (pg. 7, paragraph 5, "When a client...", line 1)

With respect to claim 30, Niemi discloses a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server (pg. 7, paragraph 5, "When a client.."; pg. 8, paragraph 1, "The AUTN token..")

With respect to claim 31, Niemi discloses authenticating the UE at the authentication node and returning an authentication result to the remote server (pg. 5, paragraph 5, "Using the shared secret..", lines 2-5; paragraph 6, "The authentication response")

With respect to claims 32-33, the claim limitations of claim 32-33 are similar to the limitations of claim 1. The only difference is a subsequent request to access the server; however the steps are the same.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esther Benoit whose telephone number is 571-270-3807. The examiner can normally be reached on Monday through Friday between 7:30 a.m and 5 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E.B.
December 1, 2009

/Shawki S Ismail/
Primary Examiner, Art Unit 2455